

USER AUTHENTICATION METHOD AND SYSTEM USING BIOLOGICAL INFORMATION AND DATA RECORDING MEDIUM, AND PROGRAM RECORDING MEDIUM

Publication number: JP2002132731

Publication date: 2002-05-10

Inventor: ITAKURA HIROKAZU; OKADA KENICHI; UENO KEIJI

Applicant: HITACHI SYSTEMS & SERVICES LTD

Classification:

- international: G06F15/00; H04L9/32; G06F15/00; H04L9/32; (IPC1-7):
G06F15/00; G06F17/60; H04L9/32

- european:

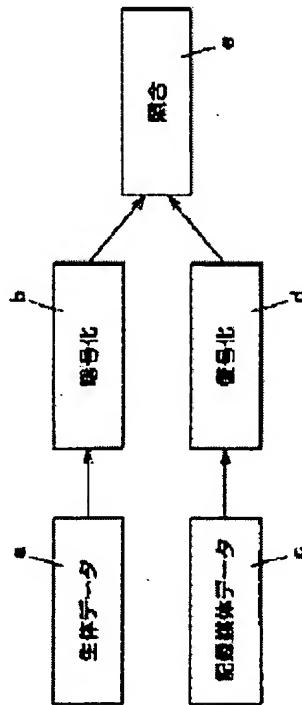
Application number: JP20000322394 20001023

Priority number(s): JP20000322394 20001023

[Report a data error here](#)

Abstract of JP2002132731

PROBLEM TO BE SOLVED: To make a user authentication system high in security level.
SOLUTION: In order to authenticate a user, biological data (a) are acquired from the user and by enciphering (b) these data, collation data on one side are generated. On the other hand, parallel with the acquisition of the biological data (a), previously enciphered data (c) are read out of a data recording medium, that the user has, and by deciphering (d) these data, collation data on the other side are generated. It is collated (e) whether these collation data are equal or not. Thus when both the data are equal to each other, the user is authenticated as a authorized user.



JP2002001

Data supplied from the [esp@cenet](#) database - Worldwide

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-132731

(P2002-132731A)

(43)公開日 平成14年5月10日(2002.5.10)

(51)Int.Cl.⁷
G 0 6 F 15/00
17/60
H 0 4 L 9/32

識別記号
3 3 0
5 1 2

F I
G 0 6 F 15/00
17/60
H 0 4 L 9/00

テ-マコ-ト(参考)
3 3 0 F 5 B 0 8 5
3 3 0 E 5 J 1 0 4
5 1 2
6 7 3 C
6 7 3 D

審査請求 未請求 請求項の数10 O L (全 12 頁) 最終頁に続く

(21)出願番号

特願2000-322394(P2000-322394)

(22)出願日

平成12年10月23日(2000.10.23)

(71)出願人 391002409

株式会社 日立システムアンドサービス
東京都大田区大森北3丁目2番16号

(72)発明者 板倉 博和

大阪府大阪市中央区内本町2丁目4番16号
株式会社日立システムアンドサービス内

(72)発明者 岡田 健一

大阪府大阪市中央区内本町2丁目4番16号
株式会社日立システムアンドサービス内

(74)代理人 100092956

弁理士 古谷 栄男 (外2名)

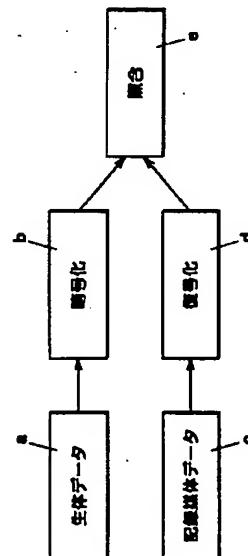
最終頁に続く

(54)【発明の名称】 生体情報とデータ記録媒体を用いたユーザ認証方法、認証装置およびプログラム記録媒体

(57)【要約】

【目的】利用者の認証システムにおいて、セキュリティレベルの高い認証システムを提供する。

【構成】利用者の認証を行うために、利用者から生体データaを取得し、これを暗号化bすることで片方の照合データを生成する。一方、生体データaを取得すると並行して、利用者が有するデータ記録媒体から予め暗号化されたデータcを読み出し、これを復号化dすることで、もう片方の照合データを生成する。これらの照合データが同一のものであるか否かを照合eする。その結果、両データが同一である場合には、正当な利用者であるとの認証がなされる。



【特許請求の範囲】

【請求項 1】利用者の生体情報を少なくとも一回暗号化した第1の暗号化生体データを予め記録したデータ記録媒体から、当該第1の暗号化生体データを読み出す読出手段と、
利用時において、利用者からその生体情報を取得する生体情報取得手段と、
生体情報取得手段からの生体情報を少なくとも一回暗号化して第2の暗号化生体データを得るとともに、読出手段によって読み出した第1の暗号化生体データに基づいて得た第3の暗号化生体データと、第2の暗号化生体データとを比較照合する照合手段と、
を備えたことを特徴とする認証装置。

【請求項 2】利用者の生体情報を少なくとも一回暗号化した第1の暗号化生体データを予め記録したデータ記録媒体から、当該第1の暗号化生体データを読み出し、
利用時において、利用者からその生体情報を取得し、
当該利用者から取得した生体情報を少なくとも一回暗号化して第2の暗号化生体データを得るとともに、データ記録媒体から読み出した第1の暗号化生体データに基づいて得た第3の暗号化生体データと、第2の暗号化生体データとを比較照合する処理を認証装置に実行させるためのプログラム、
を記録したことを特徴とするプログラム記録媒体。

【請求項 3】請求項1の認証装置又は請求項2のプログラム記録媒体において、
前記第3の暗号化生体データとして、前記第1の暗号化生体データをそのまま用いることを特徴とするもの。

【請求項 4】請求項1の認証装置又は請求項2のプログラム記録媒体において、
前記第1の暗号化生体データは、利用者の生体情報を2重に暗号化しており、
前記第3の暗号化生体データは、前記第1の暗号化生体データを1回復号化したものであることを特徴とするもの。

【請求項 5】請求項4の認証装置又はプログラム記録媒体において、
前記第1の暗号化生成データは、利用者の生体情報を第1の非対称鍵で二重に暗号化しており、
前記第3の暗号化生成データは、当該第1の暗号化生成データを第2の非対称鍵で1回復号化したものであることを特徴とするもの。

【請求項 6】請求項5の認証装置又はプログラム記録媒体において、
前記データ記録媒体は、さらに、第1の非対称鍵データおよび第2の非対称鍵を共通鍵を用いて少なくとも1回暗号化した暗号化非対称鍵データを記録しており、
前記第3の暗号化生成データは、認証時に利用者から取得したデータに基づいて生成した前記共通鍵を用いて当該暗号化非対称鍵データを1回復号化して生成する第2

の非対称鍵を用いて、前記第1の暗号化生成データを復号化することにより得ることを特徴とするもの。

【請求項 7】利用者の生体情報を記録したデータ記録媒体であって、
少なくとも生体情報を2重暗号化して記録したことを特徴とするもの。

【請求項 8】利用者の生体情報を記録したデータ記録媒体であって、
少なくとも生体情報を第1の非対称鍵で2重暗号化したデータ、第1の非対称鍵データ、第2の非対称鍵を少なくとも1回暗号化したデータを記録したことを特徴とするもの。

【請求項 9】請求項7または請求項8のデータ記録媒体において、
前記データ記録媒体は、電子透かしを組み込んだ識別子を備えたことを特徴とするもの。

【請求項 10】利用者の生体情報を少なくとも一回暗号化した第1の暗号化生体データをデータ記録媒体に予め記録しておき、
利用時においては、前記データ記録媒体から第1の暗号化生成データを読み出すとともに、利用者からその生体情報を取得し、
当該利用者から取得した生体情報を少なくとも一回暗号化して第2の暗号化生体データを得るとともに、データ記録媒体から読み出した第1の暗号化生体データに基づいて得た第3の暗号化生体データと、第2の暗号化生体データとを比較照合すること、
を特徴とする利用者の認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、システムを利用する利用者の認証技術に関し、特に、そのセキュリティーレベルの向上に関する。

【0002】

【従来の技術】近年、コンピュータシステムの発展により、産業の活性化や社会の利便性の拡大が進む反面、データ侵害やプライバシー侵害などのコンピュータ犯罪も増加するなど、その弊害も問題視されつつある。このような、犯罪行為から保護すべき対象となるべき情報は、企業利益に関わるもの、銀行業務など金融、決済に関わるもの、個人の情報に関わるものなど多様化してきている。

【0003】このような保護すべき情報を悪意の第三者による犯罪行為から守るための技術は、一般に、情報セキュリティ技術と呼ばれる。情報セキュリティ技術は、第三者の不正行為の形態によって、認証技術、アクセス制御技術、隔離技術、監視技術などに分類することができる。この発明は、特に認証技術に関するものである。

【0004】認証技術は、利用者が正当であるか否かを

確認すること（利用者認証）を目的とする情報セキュリティ技術である。利用者認証には、パスワードによる認証が用いられることが多い。しかし、パスワードのみを用いた認証では、利用者の記憶に依存するため、あまり多くの文字のパスワードを用いることができないという制限がある。このため、これとは別に利用者個人の属性情報を用いた認証や、利用者の所有物による認証が用いられている。

【0005】個人の属性情報を用いた認証では、指紋、声紋、筆跡、網膜の眼紋を属性情報とし、これを比較照合する方式が考えられている。また、所有物による認証では、印鑑の印影の比較照合があるが、最近ではICカードが多く用いられている。

【0006】なお、指紋を用いた個人認証方法は、その他の属性情報を用いた認証方法よりも確実な認証手段であり、世界中の国々で警察の分野を中心に利用されている。指紋の特徴は、隆線の指全体における流れのパターンによって表され、判別方法としては、尖点、デルタ点、渦点などの特徴点を検出し、その数と位置関係によって分類する方法などがある。

【0007】また、さらに個人の属性情報と所有物による認証を組み合わせることでセキュリティレベルを高めた方式も存在する。例えば、指紋データを認証時に入力し、ICカードに利用者の当該指紋データを記録しておき両データを比較照合する認証方式が該当し、実際にはコンピュータ室などへの入退管理用として利用されている。

【発明が解決しようとする課題】しかし、このような従来の生体情報（個人の属性情報）とデータ記録媒体（個人の所有物）の組み合わせによるユーザ認証方式では、データ記録媒体から読み出した生体情報に基づくデータと、認証時に認証装置に入力した生体情報に基づくデータとを単に比較することにより利用者の認証が行われていた。

【0008】このため、データ記録媒体や認証装置に記録された認証データの解読や、これによるデータ記録媒体の捏造、認証データの悪用などが比較的容易に実施される危険性があった。

【0009】また、ネットワーク上のサーバ側にもユーザ認証情報を記録しておくような場合には、認証情報データの改竄、成り済ましによるシステム破壊などの驚異にもさらされる可能性があった。

【0010】

【課題を解決するための手段および発明の効果】（1）この発明の認証装置は、利用者の生体情報を少なくとも一回暗号化した第1の暗号化生体データを予め記録したデータ記録媒体から、当該第1の暗号化生体データを読み出す読出手段と、利用時において、利用者からその生体情報を取得する生体情報取得手段と、生体情報取得手段からの生体情報を少なくとも一回暗号化して第2の暗

号化生体データを得るとともに、読出手段によって読み出した第1の暗号化生体データに基づいて得た第3の暗号化生体データと、第2の暗号化生体データとを比較照合する照合手段と、を備えたことを特徴とする。

【0011】したがって、データ記録媒体に生体情報を暗号化して登録することにより、元の生体情報の解読を困難にすることができます。このため、第三者がデータ記録媒体を捏造することを防止することができる。

【0012】また、暗号化した状態で比較照合するため第三者が認証のためのデータを特定し、盗用することが困難となる。

【0013】さらに、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができる。このため、セキュリティーレベルの高いシステムを構築することができる。

【0014】（2）この発明のプログラム記録媒体は、利用者の生体情報を少なくとも一回暗号化した第1の暗号化生体データを予め記録したデータ記録媒体から、当該第1の暗号化生体データを読み出し、利用時において、利用者からその生体情報を取得し、当該利用者から取得した生体情報を少なくとも一回暗号化して第2の暗号化生体データを得るとともに、データ記録媒体から読み出した第1の暗号化生体データに基づいて得た第3の暗号化生体データと、第2の暗号化生体データとを比較照合する処理を認証装置に実行させるためのプログラム、を記録したことを特徴とする。

【0015】したがって、データ記録媒体に生体情報を暗号化して登録することにより、元の生体情報の解読を困難にすることができます。このため、第三者がデータ記録媒体を捏造することを防止することができる。

【0016】また、暗号化した状態で比較照合するため第三者が認証のためのデータを特定し、盗用することが困難となる。

【0017】さらに、利用者の認証を読出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【0018】（3）この発明は、前記第3の暗号化生体データとして、前記第1の暗号化生体データをそのまま用いることを特徴とする。

【0019】したがって、認証時に必要な暗号化等の処理を可能な限り簡素にしつつ、セキュリティーレベルの高いシステムを構築することができる。

【0020】（4）この発明は、前記第1の暗号化生体

データは、利用者の生体情報を2重に暗号化しており、前記第3の暗号化生体データは、前記第1の暗号化生体データを1回復号化したものであることを特徴とする。

【0021】したがって、認証時に常に暗号化および復号化を行うことで照合の際のアルゴリズムが複雑となる。このため、セキュリティーレベルの高いシステムを構築することができる。

【0022】(5) この発明は、前記第1の暗号化生成データは、利用者の生体情報を非対称鍵で二重に暗号化しており、前記第3の暗号化生成データは、当該第1の暗号化生成データを非対称鍵で1回復号化したものであることを特徴とする。

【0023】したがって、認証時に常に非対称鍵により暗号化および復号化を行うことで照合の際のアルゴリズムが複雑となる。このため、セキュリティーレベルの高いシステムを構築することができる。

【0024】(6) この発明は、前記データ記録媒体は、さらに、第1の非対称鍵データおよび第2の非対称鍵を共通鍵を用いて少なくとも1回暗号化した暗号化非対称鍵データを記録しており、前記第3の暗号化生成データは、認証時に利用者から取得したデータに基づいて生成した前記共通鍵を用いて当該暗号化非対称鍵データを1回復号化して生成する第2の非対称鍵を用いて、前記第1の暗号化生成データを復号化することにより得ることを特徴とする。

【0025】したがって、認証時に常に非対称鍵により暗号化および復号化を行うことで照合の際のアルゴリズムが複雑となる。このため、セキュリティーレベルの高いシステムを構築することができる。

【0026】(7) この発明のデータ記録媒体は、利用者の生体情報を記録したデータ記録媒体であって、少なくとも生体情報を2重暗号化して記録したことを特徴とする。

【0027】したがって、利用者の認証を読み出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【0028】(8) この発明は、利用者の生体情報を記録したデータ記録媒体であって、少なくとも生体情報を第1の非対称鍵で2重暗号化したデータ、第1の非対称鍵データ、第2の非対称鍵を少なくとも1回暗号化したデータを記録したことを特徴とする。

【0029】したがって、利用者の認証を読み出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防

止することができ、セキュリティーレベルの高いシステムを構築することができる。

【0030】(9) この発明は、利用者の生体情報を記録したデータ記録媒体であって、前記データ記録媒体は、電子透かしを組み込んだ識別子を備えたことを特徴とする。

【0031】したがって、データ記録媒体の真贋を容易に判断することができ、媒体の捏造防止を強化することができる。

【0032】(10) この発明の利用者の認証方法は、利用者の生体情報を少なくとも一回暗号化した第1の暗号化生体データをデータ記録媒体に予め記録しておき、利用時においては、前記データ記録媒体から第1の暗号化生成データを読み出すとともに、利用者からその生体情報を取得し、当該利用者から取得した生体情報を少なくとも一回暗号化して第2の暗号化生体データを得るとともに、データ記録媒体から読み出した第1の暗号化生体データに基づいて得た第3の暗号化生体データと、第2の暗号化生体データとを比較照合すること、を特徴とする。

【0033】したがって、データ記録媒体に生体情報を暗号化して登録することにより、元の生体情報の解読を困難にすることができます。このため、第三者がデータ記録媒体を捏造することを防止することができる。

【0034】また、暗号化した状態で比較照合するため、第三者が認証のためのデータを特定し、盗用することが困難となる。

【0035】さらに、利用者の認証を読み出装置と生体情報取得手段の組み合わせにより認証装置のみで実行することができる。このため、不正利用者によるサーバへのアクセスやネットワークへの侵入を認証装置でのチェックにより拒否し、システムへの不正侵入を未然に防止することができ、セキュリティーレベルの高いシステムを構築することができる。

【0036】

【発明の実施の形態】【発明の概要について】まず、図1を用いて、この発明の概要について説明する。

【0037】この発明は、データ記録媒体を用いてユーザ認証を行うものである。したがって、ユーザ認証を受ける利用者には、認証に用いられるデータ記録媒体が予め配布されている。このデータ記録媒体には、例えば、指紋などの生体データを2重暗号化したデータ（記録媒体データc）が記録されている。

【0038】以下に、このデータ記録媒体を有する利用者がユーザ認証を受ける際に、認証装置において行われる処理について説明する。

【0039】まず、図1に示すように、生体情報取得手段は、認証時に利用者から生体データaを取得し、これを1重暗号化bする処理を行う。これにより、一方の照合データ（第2の暗号化生体データ）が生成される。

【0040】その一方で、読み出手段は、データ記録媒体から前述した2重暗号化された記録媒体データ（第1の暗号化生体データ）cを読み出し、さらに、このデータを復号化し、1重暗号化したデータに戻す処理を行う。これにより、もう一方の照合データ（第3の暗号化生体データ）が生成される。

【0041】照合手段は、これらの一重暗号化された照合データ（第2および第3の暗号化生体データ）が同じであるか否かを照合する処理を行う。その結果、両データが同一である場合には、正当な利用者であると認証し、認証装置のセキュリティ保護状態が解除される。

【0042】このように、照合を暗号化した状態で行うことにより、第三者によるデータの特定、盗用が困難となり、セキュリティーレベルを高めることが可能となる。

【0043】以下に、生体情報として利用者の指紋を用い、データ記録媒体としてICカードを用いた場合の実施形態について説明する。

【0044】[実施形態の概要について]図2は、この発明の実施形態の概念図である。

【0045】ユーザ認証を受ける利用者には、認証に用いられるICカードが予め配布されている。なお、このICカードには、指紋データfを公開鍵P（第1の非対称鍵）によって二重の暗号化したデータP[P[f]]、公開鍵データP、パスワードWに基づいて生成した共通鍵Wcによって秘密鍵S（第2の非対称鍵）を暗号化したデータWc[S]が、予め記録されている。なお、P[f]は、データfをデータPを用いて暗号化処理したことを意味する。

【0046】以下に、このICカードを有する利用者が、認証を受ける際に認証装置において行われる処理について説明する。

【0047】図2に示すように、生体情報取得手段は、まず、指紋から指紋データf'を採取する。さらに、この指紋データf'は、ICカードより読み出した公開鍵Pによって暗号化処理され、データP[f']になる。この一重暗号化処理したデータP[f']が、比較照合される一方の照合データとなる。

【0048】一方で、認証を受ける利用者は、パスワードWを入力する。認証装置では、このパスワードWに基づいて生成した共通鍵Wcによって、図2に示すように、ICカードより読み出したデータWc[S]（共通鍵Wcによって秘密鍵Sを予め暗号化したデータ）が復号化処理され、秘密鍵Sが生成される。

【0049】さらに、この生成された秘密鍵Sによって、ICカードより読み出したデータP[P[f']]を復号化処理しP[f']とする。この一重暗号化したデータP[f']が、比較照合される、もう一方の照合データとなる。

【0050】照合手段は、上記処理により生成された照合データP[f']（指紋から採取したデータに基づいて生成された一重暗号化データ）と照合データP[f]（データ記録

媒体から読み出したデータに基づいて生成された一重暗号化データ）を照合する。その結果、両データが同一であれば利用者として認証し、認証装置におけるセキュリティ保護状態は解除される。一方、両データが同一でなければ利用者として認証されないため、認証装置のセキュリティ保護状態は解除されないことになる。

【0051】[システム構成]以下に、図3および図4を用いて、この発明の一実施形態のシステム構成について説明する。なお、図3は、この発明をネットワーク利用者の認証に用いた場合のシステム構成を示す。図4は、認証装置の構成を示す図である。

【0052】図3に示すように、この発明を実施するためのシステムは、ネットワーク3を介してサーバ1と複数の認証装置であるクライアントPC5が相互に通信可能なように接続されたものとなっている。

【0053】サーバ1には、盗用などの犯罪行為から保護すべきデータが記録されている。例えば、企業利益に関わるもの、銀行業務など金融、決済に関わるもの、個人の情報に関わるものなどである。

【0054】ネットワーク3には、LAN、インターネットなどの通信手段が用いられる。

【0055】認証装置であるクライアントPC5は、図4に示すように、CPU20、メモリ22、ディスプレイ24、ハードディスク26、キーボード/マウス28、読み出手段であるICカードリーダ30、生体情報取得手段である指紋データリーダ34を備える。

【0056】クライアントPC5のハードディスク26には、マイクロソフト社のウンドウズなどのオペレーションシステム(OS)がインストールされている。また、照合手段である照合ソフトも、ハードディスク26にインストールされている。

【0057】この照合ソフトは、認証データを比較照合することで正当な利用者であるか否かを判断する処理を行う機能だけでなく、非対称鍵方式、共通鍵方式を用いたデータの暗号化および復号化処理を行う機能を備える。CPU20は、この暗号化および復号化処理などに必要な演算を行う。

【0058】なお、非対称鍵方式とは、対になる2つの鍵を使ってデータの暗号化・復号化を行なう暗号方式のことであり、公開鍵方式とも呼ばれるものである。片方は他人に広く公開するため公開鍵と呼ばれ、もう片方は本人だけがわかるよう厳密に管理されるため秘密鍵と呼ばれる。秘密鍵で暗号化されたデータは対応する公開鍵でしか復号できず、公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できない。このため鍵を安全な経路で輸送する必要がなく、共通鍵暗号方式に比べて鍵の管理が楽で安全性が高い。具体的な暗号化方式としては、巨大な整数の素因数分解の困難さを利用したRSA方式などがある。

【0059】これに対して、共通鍵方式とは、暗号化と

復号化と同じ鍵を用いる暗号方式をいう。このため、暗号文を送受信する前に、あらかじめ安全な経路を使って秘密の鍵を共有する必要がある。代表的な共通鍵暗号としては、DES、FEAL、MISTY、IDEA、などの方式がある。読み出手段であるICカードリーダ30は、ICカード32のICチップなどに記録された認証のためのデータ（認証データ）を読み出す機能を備える。

【0060】データ記録媒体であるICカード32には、認証データが記録できるICチップが組み込まれている。このICチップには、利用者の生体情報に基づくデータなどが予め記録されている。

【0061】また、このICカード32は、偽造防止のために電子透かしを組み込んだホログラムなどの識別子を備える。電子透かしとは、画像や音声を損なわない範囲で直接画像や音声データに別の情報を書き込む技術であり、ここではICカード32の真贋の判断に利用される。

【0062】生体情報取得手段である指紋データリーダ34は、クライアントPC5の利用時において利用者からその指紋情報を取得する機能を備える。具体的な、指紋データリーダ34としては、ソニーの「Sony Finger print Identification UnitFIU-700」、富士通の「Fing sensor FS-200P」などを用いることができる。

【0063】[ICカードに認証データを記録する処理]前述したように、この実施形態においては認証時にICカードがデータ記録媒体として用いられる。したがって、ユーザ認証を行うためには、ICカードを作成し、ユーザ認証を受ける利用者に対して予め配布しておく必要がある。

【0064】以下に、図5および図6を用いて、この認証に用いるデータを記録するICカードを作成する手順について説明する。なお、図5は、ICカードを生成するICカード生成装置の構成を示した図である。図6は、認証に用いるデータをICカードに認証データを記録するまでの処理を示すフローチャートである。

【0065】図5に示すように、ICカード生成装置は、CPU20、メモリ22、ディスプレイ24、ハードディスク26、キーボード／マウス28、ICカードライタ31、生体情報取得手段である指紋データリーダ34を備える。

【0066】ICカードライタ31は、ICカード32の記憶部に、認証データを書き込む機能を備える。また、ICカード生成装置のハードディスク26には、データを暗号化および復号化処理する暗号ソフトがインストールされている。CPU20は、これらの暗号化および復号化などの処理に必要な演算を行う。

【0067】まず、認証を受けようとする利用者は、ICカード生成装置の指紋データリーダ34に指を触れる。これによって、指紋データリーダ34は、図6に示すように、指紋の読み込みを開始する（ステップS101）。さらに、指紋データリーダ34は、指紋の特徴を

抽出して、指紋データfを生成する（ステップS103）。ここでは、指紋というアナログデータからデジタルデータを生成する処理が行われる。

【0068】この指紋データfを取得するための処理は、一定のアルゴリズムによって行われる。例えば、一般的に隆線の開始点、分岐点などのマイニューシャ（minutiae）の特徴からデータを取得することによりおこなわれる。なお、マイニューシャは、一指に平均100個あり、二つの指紋の間で12個以上のマイニューシャが一致すれば、同一人同一指の指紋と断定することができるとされている。従って、ここで取得される指紋データが、12個以上のマイニューシャの特徴に基づくデータであれば、利用者の認証において十分な認識率を得ることができることになる。

【0069】指紋から指紋データfを生成する具体例について、以下に説明する。

【0070】まず、指紋データリーダ34で光学的走査により指紋パターンを取り入れ、これにフィルタ処理を施してから二値化する。さらに、二値化パターンを骨格化してマイニューシャを検出する。このとき、特徴点周辺の隆起線の形状を計測して、その結果から類似特徴点を排除する。最終的に抽出された特異点について、ある特徴点（親特徴点）の周囲で4個の子特徴点を選び、親特徴点の位置（x、y）、方向（d）、子特徴点との関係（R1、R2、R3、R4）によって指紋の特徴データを生成する。すなわち、この場合の一指の特徴データは（ x^i 、 y^i 、 d^i 、 $R1^i$ 、 $R2^i$ 、 $R3^i$ 、 $R4^i$ ）（ $i=1, 2, \dots, N$ ）のセットとなり、指紋データfはこれらを組み合わせて羅列するなどによって生成することができる。

【0071】このセットの数は、少なくとも同一人の同一指と判断できる程度の数が必要となる。また、リレーションRは、皮膚の変形を考慮して特徴点間の隆線の数を用いることで不变な量とする。

【0072】指紋データfを生成した後、ICカード生成装置のハードディスク26にインストールした暗号ソフトは、1組の非対称鍵を生成する（ステップS105）。すなわち、ここで、第1の非対称鍵である公開鍵Pと、第2の非対称鍵である秘密鍵Sが生成される。なお、非対称鍵の生成方法としては、べき乗除余タイプ暗号であるRSA方式を用いる。RSA方式は、最も代表的な非対称鍵方式であり、大きな整数の因数分解の困難さを利用したことを特徴とする。

【0073】なお、この実施形態においては非対称鍵にRSA方式を採用しているが、RSA方式は、鍵によるデータ処理が一方向となっており、暗号化、復号化の方向がない。このため、RSA方式では、公開鍵で暗号化し、さらに秘密鍵で暗号化することは元のデータに戻すことと同じになってしまう。ただし、公開鍵（秘密鍵だけでも可）だけで、複数回の暗号化処理を行うことはできる。

【0074】つぎに、利用者は、自己のパスワードWを

キーボード28を介して入力する。ICカード作成装置は、このパスワードWをメモリ22に読み込む（ステップS107）。

【0075】ハードディスク26に記録した暗号ソフトは、このパスワードWを種データとして共通鍵Wcを生成する処理を行う（ステップS109）。なお、ここで生成する共通鍵Wcは、パスワードWによって一義的に定まるものとする。

【0076】さらに、暗号ソフトは、この共通鍵Wcによって秘密鍵S（ステップS105において生成済）を暗号化処理する。これにより、パスワードWに基づいて生成した共通鍵Wcによって暗号化したデータWc[S]が生成される（ステップS111）。なお、ここで用いるパスワードは、利用者が予め設定しておいたものを用いる。

【0077】また、共通鍵Wcの生成方式としては、代表的なブロック暗号タイプであるDES方式を用いる。ブロック暗号とは、平分をブロック化し、ブロックごとに暗号変換を施すタイプの暗号であり、例えば、換字法（文字を他の文字で置き換える方法）、転字法（文字の順序を入れ換える方法）などが存在するが、ここでは、これらを組み合わせたものが用いられる。

【0078】つぎに、暗号ソフトは、公開鍵P（ステップS105において生成済）を用いて、指紋データfを暗号化し、公開鍵によって暗号化したデータP[f]を生成する（ステップS113）。このデータP[f]を、さらに公開鍵Pによって暗号化処理し、P[P[f]]を生成する（ステップS115）。

【0079】このように、指紋データfを公開鍵Pを用いて二重に暗号化することによってデータP[P[f]]が生成される。なお、このデータP[P[f]]が、データ記録媒体に記録される第1の暗号化生体データである。

【0080】ICカードライタ31は、挿入されたICカード32に、前述した公開鍵Pによって2重暗号化したデータP[P[f]]（ステップS115において生成済）に加えて、公開鍵P（ステップS105において生成済）および共通鍵Cによって暗号化したデータW[S]（ステップS111において生成済）を記録する。

【0081】以上の処理によって、ICカードは作成される。このICカードは、システム管理者によって利用者に対して配布される。例えば、この発明を銀行のATMにおけるキャッシュカードを用いた現金の取り扱いに用いた場合は、銀行がICカード32を上記のようにして作成し、利用者に対して配布する。

【0082】利用者は、以下に説明するように、ユーザ認証時にこのICカード32を用いることとなる。

【0083】【利用者の認証手順】以下に、図7及び図4を用いて、上記のように作成したICカード32を用いた認証の手順について説明する。なお、図7は、利用者の認証手順を示したフローチャートである。

【0084】まず、ユーザ認証を受けようとする利用者

は、クライアントPC5の指紋データリーダ34に指を触れる。これによって、指紋データリーダ34は、指紋の読み込みを開始する（ステップS201）。さらに、クライアントPC5の指紋データリーダ34は、指紋の特徴を抽出して、指紋データf'を生成する（ステップS203）。ここでは、前述したICカード作成時における指紋データの作成方法において説明したのと同様のデジタルデータ生成処理（図6のステップS103における処理）が行われる。

【0085】その一方で、利用者は、図4に示すクライアントPC5のICカードリーダ30に自己のICカード32を挿入する。これにより、ICカードリーダ30は、ICカード32に記録された公開鍵データPを読み出す（ステップS205）。さらに、照合ソフトは、この公開鍵データPを用いて、ステップS203で生成した指紋データf'を暗号化処理し、データP[f']を生成する（ステップS207）。なお、このデータP[f']が、後に比較照合される一方の照合データ（第二の暗号化生体データ）であり、メモリ22に記録される。なお、ICカードリーダ30は、同時にICカード32が備えるログラムから電子透かしデータを読み取り、ICカード32の真贋を判断する。

【0086】つぎに、利用者は、キーボード／マウス28を介してクライアントPC5にパスワードWを入力する。これにより、クライアントPC5は、パスワードWのデータを取得する（ステップS209）。なお、ここで入力するパスワードは、当然に前述のICカード作成時において（図5のステップS107）入力したパスワードと同じものを用いる。このパスワードWを用いて、ステップS109における処理（図5参照）と同様にDES方式により共通鍵Wcが生成される。

【0087】また、クライアントPC5のICカードリーダ30は、ICカード32に記録されたデータWc[S]を読み出す（ステップS211）。さらに、照合ソフトは、この共通鍵Wcを用いて、ICカード32から読み出したデータWc[S]を復号化し、元の秘密鍵Sの状態にもどす（ステップS213）。

【0088】つぎに、クライアントPC5のICカードリーダ30は、ICカード32に記録されたデータP[P[f]]を読み出す（ステップS215）。なお、データP[P[f]]は、公開鍵Pによって指紋データfを2重に暗号化したものである。

【0089】さらに、照合ソフトは、この復号化した秘密鍵Sを用いて、ICカード32から読み出したデータP[P[f]]を復号化処理し、一重に暗号化したデータP[f]の状態に戻す（ステップS217）。この一重暗号化したデータP[f]が、照合ソフトに比較照合されるもう一方の照合データ（第3の暗号化生体データ）である。

【0090】照合ソフトは、メモリ22に記録された第2の暗号化生体データP[f']（ステップS207にお

いて、指紋データリーダ34によって読み出した指紋データを暗号化処理したもの)と第3の暗号化データP[f](ICカードリーダ30によってICカード32から読み出したデータP[P[f]]をステップS217において復号化処理したもの)とを比較照合することによって両データの同一性を判断し、以下のようなユーザ認証処理を行う(ステップS219)。

【0091】比較照合の結果、両データが同一と照合手段が判断した場合は、正当な利用者として認証され、クライアントPC5におけるセキュリティ保護状態が解除される(ステップS221)。これにより、その後、クライアントPC5とサーバ1との間で通信が行うことができ、サーバ1とのアクセス実行も可能となる。

【0092】これに対し、両データが同一でないと照合ソフトが判断した場合には、正当な利用者として認証されず、クライアントPC5におけるセキュリティ保護状態が解除されない(ステップS223)。すなわち、かかる場合は、悪意の第三者による成りすましてある可能性が高いため、クライアントPC5とサーバ1との間ではアクセス実行が不可能となる。なお、このような場合は、クライアントPC5よりサーバ1に対して警告を行うことによりセキュリティ管理者に注意を促すことが望ましい。

【0093】[その他の実施形態]なお、この実施形態においては、ICカード32に記録する第1の暗号化生体データを生成するために、指紋データfを非対称鍵の1つである公開鍵Pによって二重暗号化処理することとしたが、共通鍵によって指紋データを二重暗号化することによって、第1の暗号化生体データを生成してこの発明を実施してもよい。

【0094】なお、この実施形態においては、ICカード32から読み出した第1の暗号化生体データを非対称鍵によって復号化した後、第2の暗号化生体データと比較照合することとした。しかし、第1の暗号化生体データを復号化せずに、そのまま第3の暗号化生体データとして、第2の暗号化生体データと比較照合するようにしてもよい。

【0095】例えば、この実施形態において、ICカード32には、第1の暗号化生体データとして公開鍵Pにより二重暗号化したデータP[P[f]]が記録されており、このデータがそのまま第3の暗号化生体データとして第2の暗号化生体データP[P[f]]と比較照合されるような場合が該当する。この場合、第2の暗号化生体データは、利用時に取得した指紋データf'を公開鍵Pにより二重暗号化して生成する。

【0096】また、上記のように第2および第3の暗号化生体データの比較照合は、一重暗号化した状態で行う場合に限られず、二重暗号化した状態またはそれ以上の複数回暗号化した状態で比較照合を行うようにしても良い。

【0097】なお、この実施形態においては、生体情報に指紋の情報を用いたが、その他の個人の属性情報である声紋、筆跡、網膜の眼紋などの情報を用いてもよい。

【0098】なお、この実施形態においては、非対称鍵の生成方法としてRSA方式を用いたが、DSA方式などのその他の非対称鍵の生成方法を用いてもよい。また、共通鍵生成方式として、ブロック暗号タイプであるDES方式を用いたが、ストリーム暗号タイプを用いてもよい。

【0099】なお、この実施形態においては、第1の非対称鍵として公開鍵Pを、第2の非対称鍵として秘密鍵Sを用いたが、これに限定されず、第1の非対称鍵として秘密鍵Sを、第2の非対称鍵として公開鍵Pを用いてもよい。

【0100】なお、この実施形態においては、マイニューシャの特徴に基づいて指紋データfを生成したがこれに限定されるものではなく、隆線の形状を単にビットマップデータに変換することで指紋データfを生成するようにもよい。

【0101】なお、この実施形態においては、共通鍵Wcを生成するために利用者が予め設定したパスワードWを用いたが、指紋情報などの個人の属性情報などをパスワードとして用いてもよい。

【0102】なお、この実施形態においては、データ記録媒体にICカード32を用いたが、磁気カード、USBキーなどを用いてもよい。

【0103】なお、この実施形態においては、本発明をクライアントPC5のセキュリティ状態を解除するための認証に用いたが、これに限定されず企業におけるコンピュータ室の入退管理、銀行のATMにおける口座の取り扱いなどにも用いることができる。

【0104】なお、この実施形態においてはサーバ1が存在することとしたが、サーバ1が存在しないような場合であってもよい。例えば、クライアントPC5のみが、ネットワーク3に接続されているような場合である。さらに、クライアントPC5のみにおける認証についても、この発明を用いることができる。

【図面の簡単な説明】

【図1】この発明の概要図である。

【図2】この発明の実施形態の概要図である。

【図3】この発明を実施するためのシステム構成を示す図である。

【図4】クライアントPCの構成を示す図である。

【図5】ICカード生成装置の構成を示す図である。

【図6】データ記録媒体へデータを記録するまでの手順を示すフローチャートである。

【図7】利用者の認証手順を示すフローチャートである。

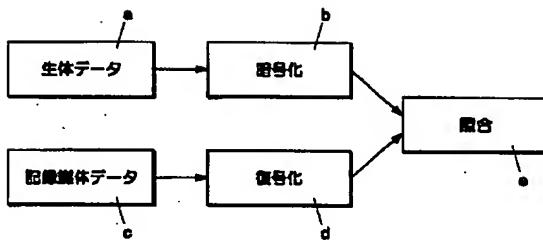
【符号の説明】

1 サーバ

3 ネットワーク

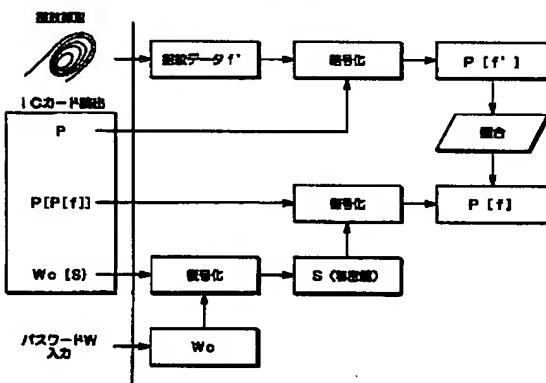
5 クライアントPC	28 キーボード/マウス
20 CPU	30 ICカードリーダ
22 メモリ	31 ICカードライタ
24 ディスプレイ	32 ICカード
26 ハードディスク	34 指紋データリーダ

【図1】

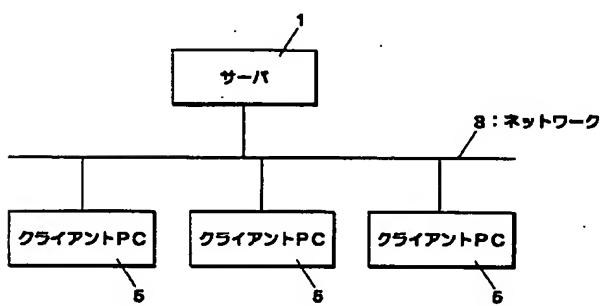


【図2】

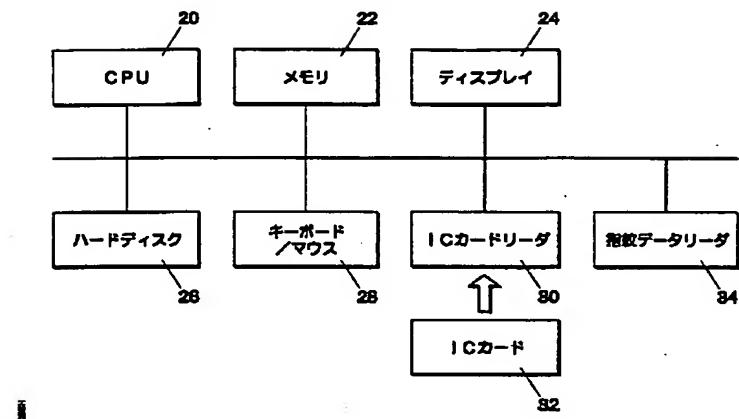
実施形態概要図



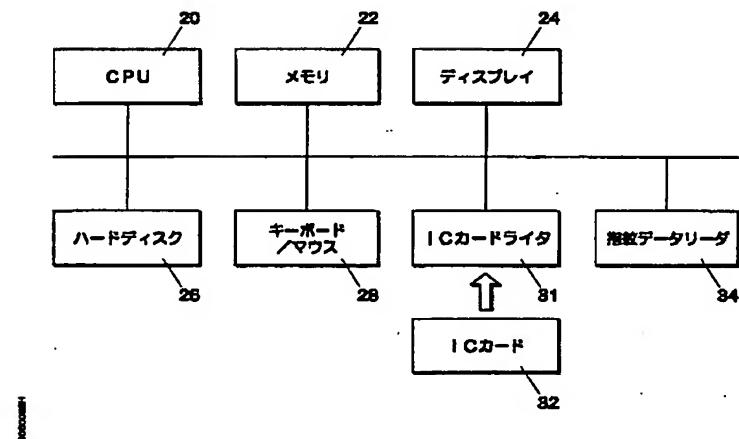
【図3】



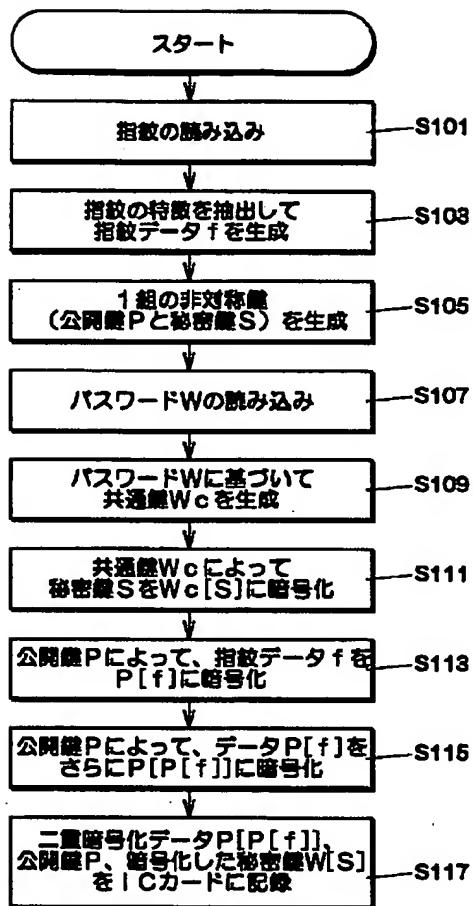
【図4】



【図5】

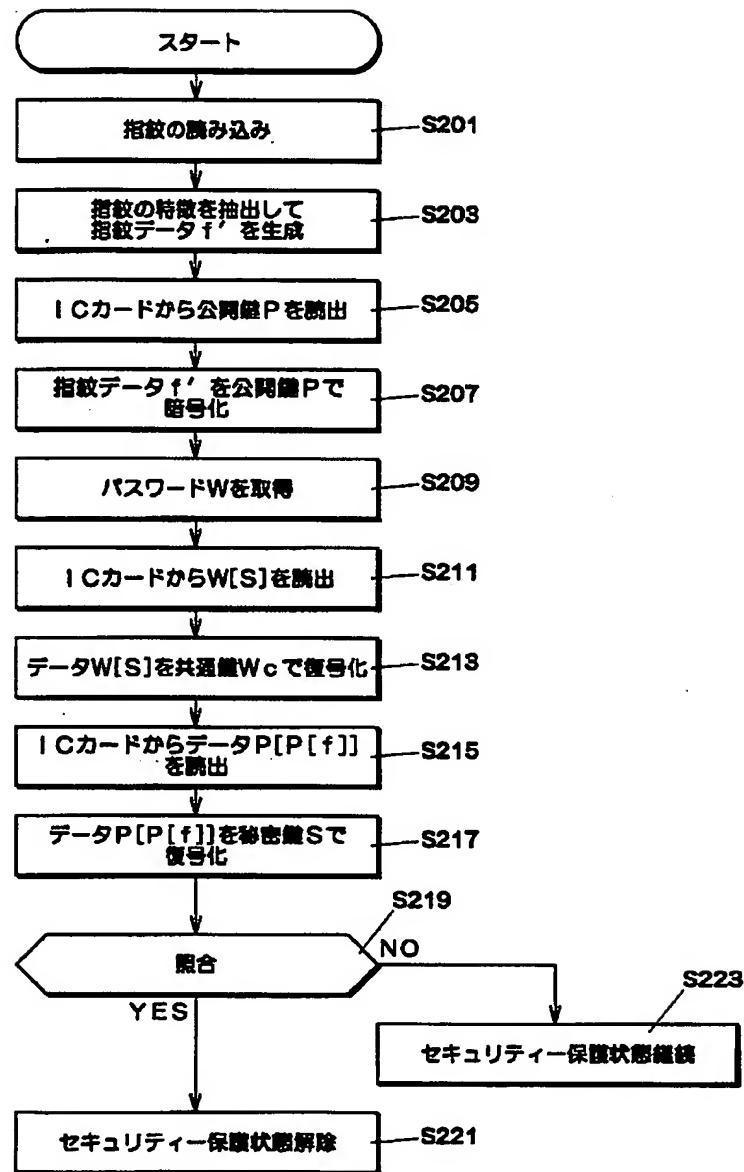


【図6】



H3300908

【図 7】



HSS00907

フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テマコード(参考)

H 0 4 L 9/00

6 7 3 E

(72) 発明者 植野 圭二

大阪府大阪市中央区内本町 2 丁目 4 番 16 号
株式会社日立システムアンドサービス内

F ターム(参考) 5B085 AE09 AE25 AE29

5J104 AA07 AA14 AA16 EA06 EA18

KA01 KA05 KA16 KA17 NA02

NA05 NA35 NA37 NA38